(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－99421
（P2000－99421A）
(43)公開日　平成12年４月７日(2000.4.7)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
G06F 13/00	351	G06F 13/00	351G	5B089
G09C 1/00	640	G09C 1/00	640B	5K030
	660		660E	
H04L 12/54		H04L 11/20	101B	
12/58				

審査請求　未請求　請求項の数12　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－267682

(22)出願日　平成10年９月22日(1998.9.22)

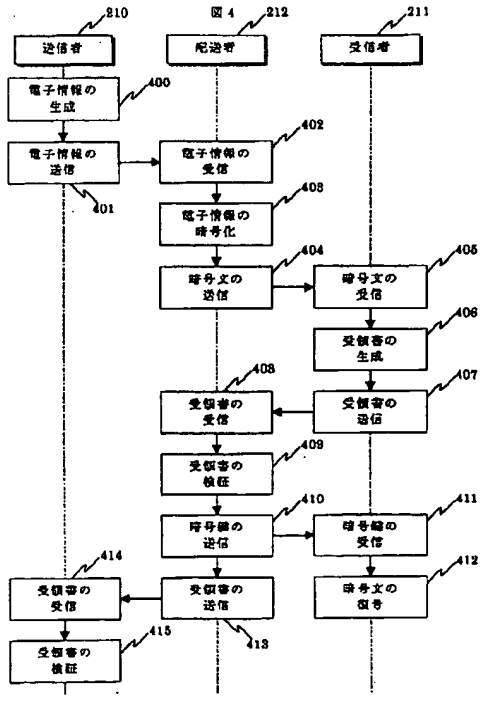
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　鍛　忠司
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100068504
弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　電子情報の到達確認方法

(57)【要約】
【課題】第一のユーザが第二のユーザに対し，ネットワークを介して電子情報を送信した場合に，第二のユーザが当該電子情報を受け取ったことを，第一のユーザが確認可能とする。
【解決手段】送信者２１０は，受信者２１１に伝達する電子情報を生成し，該電子情報と受信者２１１の宛先とを配送者２１２に送信する。配送者２１２は，ランダムに暗号鍵を生成し，該暗号鍵で受け取った電子情報を暗号化して暗号文を生成する。そして，該暗号文を受信者２１１に送信する。受信者２１１は，該暗号文を受け取ったことを示す受領書を生成した後，該受領書を配送者２１２に返送する。配送者２１２は，該受領書の正当性を検証し，該受領書が正当なものであることが確認された場合にのみ，前記暗号鍵を受信者２１１に送信するとともに，受領書を送信者２１０に送信する。受信者２１１は，受け取った暗号鍵で暗号文を復号して電子情報を復元する。

図４



1

【特許請求の範囲】

【請求項１】送信者から受信者に対して電子情報を送る場合に，送信者は，システムを利用する全てのユーザが信頼する配送者を介して前記電子情報を受信者に送信し，受信者は，該電子情報を閲覧する前に，当該電子情報を受け取ったことを保証する受領書を，前記配送者を介して送信者に送信することを特徴とする到達確認方法。

【請求項２】請求項１記載の到達確認方法であって，前記配送者は，送信者より電子情報が送られてきたら，該電子情報を受信者が直接正しい内容を知ることができないデータに変換した後，該変換データを受信者に送信し，受信者より前記変換データを受け取ったことを保証する受領書が送られてきたら，該受領書の正当性が確認できた場合にのみ，当該変換データを元の電子情報に復元するためのキーデータを受信者に送信するとともに，当該受領書を送信者に送信する，ことを特徴とする到達確認方法。

【請求項３】送信者から受信者に対して電子情報を送る場合に，送信者は，前記電子情報を受信者に送信し，受信者は，該電子情報を閲覧する前に，当該電子情報を受け取ったことを保証する受領書を送信者に送信することを特徴とする到達確認方法。

【請求項４】請求項３記載の到達確認方法であって，前記送信者は，受信者に伝達する電子情報を生成した後，該電子情報を受信者が直接正しい内容を知ることができないデータに変換した後，該変換データを受信者に送信し，受信者より前記変換データを受け取ったことを保証する受領書が送られてきたら，該受領書の正当性が確認できた場合にのみ，当該変換データを元の電子情報に復元するためのキーデータを受信者に送信する，ことを特徴とする到達確認方法。

【請求項５】請求項２および請求項４記載の到達確認方法であって，前記変換データが，前記電子情報を暗号化した暗号文であり，前記キーデータが，当該暗号文を元の電子情報に復号するための暗号鍵であることを特徴とする到達確認方法。

【請求項６】請求項２および請求項４記載の到達確認方法であって，前記変換データが，前記電子情報の閲覧可否を制御するプログラムであり，前記キーデータが，当該電子情報を閲覧可能とするための暗証コードであることを特徴とする到達確認方法。

【請求項７】請求項２記載の到達確認方法であって，前記配送者は，さらに，送信者から受信者に電子情報が送られたこと，および受信者から送信者に該電子情報に対する受領書が送られたことなどを記録した利用履歴を保管しておき，送信者や受信者から開示要求を受けた場合に，該利用履歴を送信者，あるいは受信者に送付することを特徴とする到達確認方法。

【請求項８】電子情報の送信用端末と，配送用端末と，

2

受信用端末と，が通信網を介して相互に接続されており，前記送信用端末は，受信用端末に伝達する電子情報を生成する手段と，該電子情報を配送用端末に送信する手段と，配送用端末から送られてきた前記電子情報に対する受領書を受信する手段と，を備え，前記配送用端末は，送信用端末から送られてきた電子情報や，受信用端末から送られてきた受領書を受信する手段と，前記電子情報を，受信用端末で直接閲覧することができないデータに変換する手段と，前記受領書の正当性を検証する手段と，前記変換データや，該変換データを元の電子情報に復元するために用いられるキーデータを受信用端末に送信する手段と，前記受領書を送信用端末に送信する手段と，を備え，前記受信用端末は，配送用端末から送られてきた変換データやキーデータを受信する手段と，該変換データを受け取ったことを保証する受領書を生成する手段と，前記キーデータを用いて前記変換データを元の電子情報に復元し，閲覧する手段と，前記受領書を配送用端末に送信する手段と，を備えていることを特徴とする到達確認サービスシステム。

【請求項９】電子情報の送信用端末と，受信用端末と，が通信網を介して相互に接続されており，前記送信用端末は，受信用端末に伝達する電子情報を生成する手段と，前記電子情報を，受信用端末で直接閲覧することができないデータに変換する手段と，該変換データや，該変換データを元の電子情報に復元するために用いられるキーデータを受信用端末に送信する手段と，受信用端末から送られてきた受領書を受信する手段と，該受領書の正当性を検証する手段と，を備え，前記受信用端末は，送信用端末から送られてきた変換データやキーデータを受信する手段と，該変換データを受け取ったことを保証する受領書を生成する手段と，前記キーデータを用いて前記変換データを元の電子情報に復元し，閲覧する手段と，前記受領書を配送用端末に送信する手段と，を備えていることを特徴とする到達確認サービスシステム。

【請求項１０】請求項８および請求項９記載の到達確認サービスシステムであって，前記変換データが，前記電子情報を暗号化した暗号文であり，前記キーデータが，当該暗号文を元の電子情報に復号するための暗号鍵であることを特徴とする到達確認サービスシステム。

【請求項１１】請求項８および請求項９記載の到達確認サービスシステムであって，前記変換データが，前記電子情報の閲覧可否を制御するプログラムであり，前記キーデータが，当該電子情報を閲覧可能とするための暗証コードであることを特徴とする到達確認サービスシステム。

【請求項１２】請求項８記載の到達確認サービスシステムであって，前記配送用端末は，さらに，送信用端末から受信用端末に電子情報が送られたこと，および受信用端末から送信用端末に該電子情報に対する受領書が送られたことなどを記録した利用履歴を保管する手段と，送

信用端末や受信用端末から開示要求を受けた場合に，該利用履歴を送信用端末，あるいは受信用端末に送付することを特徴とする到達確認サービスシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，ある送信者から受信者に対し，電子情報を伝達するシステムにおける電子情報の到達確認方法に関する。

【０００２】

【従来の技術】情報通信機器の発達により，様々な情報が電子化され，電子メールシステムなどを利用して，ネットワークを介してやり取りされるようになってきている。このような情報通信システムは，電話や郵便などに比べ，遠く離れた人とでも簡単，正確，かつ高速に電子情報をやり取りできるといった利点を有している。

【０００３】一般に，ネットワークを介して電子情報をやり取りする場合，以下に示すような2つの課題がある。

【０００４】一つは，セキュリティに関する問題である。前記情報通信システムでは，遠く離れた相手と非対面で情報のやり取りを行うため，　送信者は，受信者が，送信者が意図した受信者本人であるかどうかがわからない，　受信者は，送信者が自称する本人であるかどうかがわからない，　受信者は，受け取った情報が正しいものであるかどうか（ネットワーク上で不正な改ざんが加えられていないかどうか）がわからない，　送信者および受信者は，情報の機密が守られているかどうか（ネットワーク上で不正に盗聴されていないかどうか）がわからない，などといったセキュリティ上の脅威が存在する。

【０００５】このような課題に対しては，従来より暗号や認証といったセキュリティ技術を適用することで対策が図られている。具体的には，通信相手の確認や改ざん検知は，電子情報にディジタル署名を付加することで実現している。また，情報の機密保護については，電子情報を暗号化することによって実現している。上記セキュリティ技術の詳細，および電子メールシステムへの適用方法については，例えば，「ＰＧＰ：ＰＲＩＴＹ　ＧＯＯＤ　ＰＲＩＶＡＣＹ」（著者：ＳｉｍｓｏｎＧａｒｆｉｎｋｅｌ，発行所：Ｏ’Ｒｅｉｌｌｙ　＆　Ａｓｓｏｃｉａｔｅｓ，Ｉｎｃ．）に記載されている。

【０００６】ネットワークを介して電子情報をやり取りする場合のもう一つの課題は，受信者が電子情報を受け取ったことを送信者が確認できないこと，すなわち，到達確認手段がないことである。例えば，電話によって情報を伝達する場合には，直接会話しているので相手に情報が正しく伝わったかどうかをその場で確認することができる。また，郵便によって情報を伝達する場合には，現行の配達証明郵便制度を利用することにより，送信者は，受信者が情報を受け取ったことを確認することが可

能である。しかし，電子メールシステムなどを利用して電子情報を送る場合，送信者は，受信者が当該電子情報を受け取ったかどうかを確認することができない。一部の電子メールソフトには，独自に到達確認機能を実装したものもあるが，受信者が同じ電子メールソフトを使っていないと利用できなかったり，受信者が意図的に受領書を返送したりしなければならないといったものである。そのため，受信者が，電子情報を受け取ったにもかかわらず，受け取っていないと虚偽の申し出をすることも可能である。

【０００７】受信者が当該電子情報を受け取ったかどうか，また，もし受け取っていたとしたらどの時点で（いつ）受け取ったのか，ということを送信者が確認できるようにすることは，利用者の利便性を高めるだけでなく，例えば，契約文書や法的執行力を持つ文書などを伝達する場合に必要となることは容易に予想される。

【０００８】上記背景から，すでに図１に示すような到達確認サービスシステムが実用化され，一般ユーザに対してサービス提供されはじめている。図１に示す到達確認サービスシステムの概要は以下の通りである。図１において，実線の矢印は電子メールを使った通信を，点線の矢印はＷｅｂサーバとブラウザプログラムを使った通信を表している。

【０００９】まず，本システムを利用する全てのユーザは，あらかじめ電子情報の配送者（サービス提供者）１１０にサービスの利用を申し込み，ユーザ管理ファイル１１１に自分のユーザＩＤとパスワードを登録してもらうとともに，自分用のメールボックス１１２を生成してもらう。

【００１０】送信者１００が，受信者１０１に対して電子情報を送る場合，送信者１００は，送りたい電子情報と受信者の宛先情報（ユーザＩＤ）とを，配送者１１０に電子メールで送信する（ステップ１２０）。

【００１１】送信者１００からの電子情報を受け取った配送者１１０は，まず，該電子情報を受信者のメールボックス１１２に格納する。次に，送信者１１０から電子情報が送られてきている旨を，該電子情報の格納先を示すＵＲＬアドレスとともに受信者１０１に電子メールで通知する（ステップ１２１）。

【００１２】配送者１１０からの通知を受け取った受信者１０１は，ブラウザプログラムを用いて前記ＵＲＬにアクセスし，ユーザＩＤとパスワードを入力して自分の身元を証明した後（ステップ１２２），送信者１００から送られてきた電子情報をメールボックス１１２からダウンロードする（ステップ１２３）。

【００１３】配送者１１０は，受信者１０１が電子情報をダウンロードしたことを検知したら，配達完了通知を送信者１００に送信して，一連の処理を終了する（ステップ１２４）。また，もし，ある一定期間内に受信者１０１が電子情報をダウンロードしなかった場合には，当

該電子情報を送信者１００に返送するとともに，その旨を通知する。

【００１４】

【発明が解決しようとする課題】ところで，前述のようなネットワークを介した電子情報のやり取りがより頻繁に行われるようになると，前記従来の到達確認サービスシステムでは，以下のような問題が生じる。

【００１５】すなわち，前記従来の到達確認サービスシステムでは，送信者および受信者は，あらかじめ配送者にサービス利用を申し込んでおかなければならない。しかし，たくさんのユーザが様々な目的で電子情報のやり取りを行うような環境下では，ある決められた相手に対してしか到達確認サービスを利用することができないのは不便である。加えて，前記従来の到達確認サービスシステムは，電子メールとブラウザを併用するシステムであり，その他のネットワークアプリケーションを利用する場合を考慮したものとはなっていない。

【００１６】本発明は，上記事情に鑑みてなされたものであり，本発明の目的は，事前のユーザ登録などを必要とせず，第一のユーザが第二のユーザに対し，何らかのネットワークアプリケーションを用いて，ネットワークを介して電子情報を送信した場合に，第二のユーザが当該電子情報を受け取ったことを，第一のユーザが確認することができる到達確認方法，およびそれを用いたシステム，さらには，該システムで使われる個々の装置と，それらを動作させるプログラムと，を提供することである。

【００１７】

【課題を解決するための手段】上記課題を達成するために、本発明の到達確認方法では，第一のユーザから第二のユーザに対して電子情報を送る場合に，第一のユーザは電子情報をシステムを利用する全てのユーザが信頼する第三者（第三者機関）を介して第二のユーザに送信し，第二のユーザは該電子情報を利用する前に当該電子情報を受け取ったことを保証する受領書を第三者を介して第一のユーザに送信することを特徴とする。

【００１８】すなわち，本発明の到達確認方法では，第一のユーザから第二のユーザに対して電子情報を送る場合に，第一のユーザは電子情報をシステムを利用する全てのユーザが信頼する第三者（第三者機関）に送付する。第三者は，該電子情報を所定の方法により、すべてが揃うと該電子情報を復元できる複数の情報に再構成して，該複数の情報の一部を前記第二のユーザへ送る。該第三者は，第二のユーザから，該第二のユーザが該複数の情報の一部を確かに受け取ったことを，事後になっても証明可能な受領書が送られてきたら，該受領書の正当性を検証した後，正しい受領書であることが確認された場合に該複数の情報の残りを第二のユーザに送るとともに，第一のユーザに対して上記受領書を送ることを特徴とする。

【００１９】本発明によれば，システムを利用する全てのユーザが信頼する第三者が，第一のユーザから送られてきた電子情報を，直接利用できない形に変換してから第二のユーザに送信するようにしている。さらに，該第三者は，第二のユーザから，該第二のユーザが変換データを確かに受け取ったことを，事後になっても証明可能な受領書が送られてきたら，該受領書の正当性を検証した後，正しい受領書であることが確認された場合にのみ，上記変換データを利用可能にするために必要な情報を第二のユーザに送信するとともに，第一のユーザに対して上記受領書を送信するようにしている。

【００２０】より具体的には、上記「電子情報の利用」のより具体的な一形態として、閲覧がある。また，すべてが揃うと元の電子情報を復元できる再構成された複数の情報として，一組の，暗号化された電子情報とその復号化鍵や，一組の，所定の方法により2つ以上に分割された電子情報や，一組の，変換された電子情報とその情報を利用するために必要な専用プログラムがある。また，上記再構成された複数の情報それぞれは、データまたはプログラムであってもよい。また，上記再構成された複数の情報の送付順序は限定されない。したがって，本発明によれば，第一のユーザが第二のユーザに対し，ネットワークを介して電子情報を送信した場合に，第二のユーザが当該電子情報を受け取ったことを，第一のユーザがきちんと確認することができる。

【００２１】

【発明の実施の形態】以下，図面を用いて，本発明の実施例を説明する。なお，以下で説明する図面において，同一の番号は同様の部品・要素を表すものとする。また，これにより本発明が限定されるものではない。図２は，本発明の第一の実施形態が適用された到達確認サービスシステムの概略構成を示す図である。本実施形態の到達確認サービスシステムは，電子情報の送信者２１０と受信者２１１，および到達確認サービスを提供する配送者２１２とが利用するシステムであって，図２に示すように，端末２２０_1～２２０_3（以下，単に端末２２０とも称する）が通信網２００を介して，互いに接続された構成になっている。ここで，配送者２１２は，本発明の到達確認サービスシステムを利用する全てのユーザが信頼する第三者である。

【００２２】端末２２０_1は，送信者２１０が使用する端末である。送信者２１０は，端末２２０_1を使って，受信者２１１に伝達するための電子情報を生成したり，通信網２００を介して配送者２１２とデータのやり取りを行ったりする。端末２２０_2は，受信者２１１が使用する端末である。受信者２１１は，端末２２０_2を使って，受け取った電子情報を閲覧したり，通信網２００を介して配送者２１２とデータのやり取りを行ったりする。端末２２０_3は，配送者２１２が使用する端末である。配送者２１２は，端末２２０_3を使って，通信網２

００を介して送信者２１０や受信者２１１とデータのやり取りを行う。さらに，該データのやり取りに関する履歴を，利用履歴ファイル２３０に格納する。

【００２３】次に，本実施形態の到達確認サービスシステムを構成する端末２２０を図面を参照して詳細に説明する。図３は，端末２２０のハードウェア構成を示す図である。本実施形態の端末２２０のハードウェア構成は，図３に示すように，表示装置３０１と，入力装置３０２と，通信網インタフェース３０３と，記憶装置３０４と，中央処理装置（ＣＰＵ）３０５と，一時記憶装置（メモリ）３０６とが，バス３００によって互いに接続されて構成されている。

【００２４】表示装置３０１は，端末２２０を使用する送信者２１０，受信者２１１，あるいは配送者２１２（以下，全てを纏めて単に利用者とも称する）に各種データを表示するために用いられるものであり，ＣＲＴや液晶ディスプレイなどで構成される。入力装置３０２は，端末２２０を使用する利用者がデータや命令等を入力するために用いられるものであり，キーボードやマウスなどで構成される。通信網インタフェース３０３は，通信網２００を介して他の端末とデータのやり取りを行うためのインタフェースである。記憶装置３０４は，端末２２０で使用されるプログラムやデータを永続的に記憶するために用いられるものであり，ハードディスクやフロッピーディスクなどで構成される。前記利用履歴ファイル２３０も該記憶装置３０４に記憶されるデータの一つである。ＣＰＵ３０５は，端末２２０を構成する各部を統括的に制御したり，様々な演算処理を行ったりする。メモリ３０６には，オペレーティングシステム３０６ａ（以下，単にＯＳ３０６ａとも称する）や，アプリケーションプログラム３０６ｂ，あるいは到達確認サービスプログラム３０６ｃなどといった，ＣＰＵ３０５が上記の処理をするために必要なプログラムなどが一時的に格納される。

【００２５】ＯＳ３０６ａは，端末２２０全体の制御を行うためにファイル管理やプロセス管理，あるいはデバイス管理といった機能を実現するためのプログラムである。アプリケーションプログラム３０６ｂは，電子情報を生成，閲覧したり，通信網２００を介して他の端末とデータのやり取りを行ったりするためのプログラムである。到達確認サービスプログラム３０６ｃは，電子情報を暗号化して暗号文を生成，または該暗号文を復号して元の電子情報に復元，または受け取った暗号文に対する受領書を生成，または該受領書の正当性を検証するためのプログラムである。すなわち，送信者２１０は，到達確認サービスプログラム３０６ｃを使って，配送者２１２経由で受信者２１１より送られてきた受領書の正当性を検証する。また，受信者２１１は，到達確認サービスプログラム３０６ｃを使って，配送者２１２から送られてきた暗号文に対する受領書を生成した後，同じく配送者２１２から送られてきた暗号鍵を用いて，上記事前に受け取っていた暗号文を復号する。さらに，配送者２１２は，到達確認サービスプログラム３０６ｃを使って，ランダムに暗号鍵を生成し，該暗号鍵を用いて送信者２１０より送られてきた電子情報を暗号化するとともに，受信者２１１より送られてきた受領書の正当性を検証する。

【００２６】次に，本実施形態の到達確認サービスシステムの動作について説明する。図４は，送信者２１０が生成した電子情報を受信者２１１に送り，当該電子情報に対する受領書を受け取る場合の，送信者２１０，受信者２１１，および配送者２１２の動作を説明するための図である。ここで，受領書とは，受信者２１１が確かに電子情報を受け取ったことを保証するデータであり，例えば，受け取った暗号文の圧縮子と受け取った日時とを連結したデータに受信者のディジタル署名を付加したものである。しかし，本発明はこれに限定されず，別のデータを用いてもよい。

【００２７】図４において，送信者２１０が行う処理には端末２２０_1が使用され，受信者２１１が行う処理には端末２２０_2が使用される。また，配送者２１２が行う処理には端末２２０_3が使用される。まず，送信者２１０は，アプリケーションプログラムを使って，受信者２１１に伝達する電子情報を生成し（ステップ４００），該電子情報と受信者２１１の宛先とを配送者２１２に送信する（ステップ４０１）。電子情報を受け取った配送者２１２は（ステップ４０２），到達確認サービスプログラムを使って，ランダムに暗号鍵を生成し，該暗号鍵で受け取った電子情報を暗号化して暗号文を生成する（ステップ４０３）。次に，アプリケーションプログラムを使って，該暗号文を受信者２１１に送信する（ステップ４０４）。暗号文を受け取った受信者２１１は（ステップ４０５），到達確認サービスプログラムを使って，該暗号文を受け取ったことを示す受領書を生成した後（ステップ４０６），該受領書をアプリケーションプログラムを使って配送者２１２に返送する（ステップ４０７）。

【００２８】受領書を受け取った配送者２１２は（ステップ４０８），まず，到達確認サービスプログラムを使って，該受領書の正当性を検証する（ステップ４０９）。そして，該受領書が正当なものであることが確認された場合にのみ，アプリケーションプログラムを使って，前記暗号鍵を受信者２１１に送信するとともに（ステップ４１０），受領書を送信者２１０に送信する（ステップ４１３）。さらに，上記処理が行われたことを示す利用履歴を，利用履歴ファイルに保管する。ここで，受領書の正当性確認とは，該受領書が受信者本人によって生成されたものであること，および受信日時が妥当なものであること，などを確認することである。上記手順において，もし，あらかじめ決められた時間を経過した

後になっても受信者２１１から受領書が送られてこなかったり，また，送られてきた受領書が正当なものでなかったりした場合には，受信者２１１にその旨を連絡して受領書の送信（再送）を要求してもよいし，送信者２１０に正当な受領書が送られてこなかった旨を連絡してもよい。

【００２９】最後に，暗号鍵を受け取った受信者２１１は（ステップ４１１），到達確認サービスプログラムを使って，該暗号鍵で暗号文を復号して電子情報を復元する（ステップ４１２）。一方，受領書を受け取った送信者２１０は（ステップ４１４），到達確認サービスプログラムを使って，該受領書の正当性を検証する（ステップ４１５）。上記手順において，送信者２１０による受領書の正当性検証処理は（ステップ４１５），同様の処理を配送者２１２が行っているため，省略することも可能である。上記の本実施形態では，送信者２１０は，配送者２１２に電子情報の配送と該電子情報に対する受領書の返送を依頼するようにしている。また，配送者２１２は，送信者２１０より受け取った電子情報をランダムな暗号鍵で暗号化し，該暗号文のみを受信者２１１に送るようにしている。さらに，受信者２１１から送られてきた受領書が正当なものである場合にのみ，暗号文を復号するために必要な暗号鍵を受信者２１１に送信するようにしている。加えて，上記処理が行われたことを示す利用履歴を保管するようにしている。さらにまた，受信者２１１は，電子情報の正しい内容を知るために，配送者２１２に受領書を送信しなければならないようにしている。

【００３０】したがって，本発明によれば，送信者２１０は，配送者２１２を経由して受信者２１１からの受領書を受け取ることで，電子情報が正しい受信者２１１に送られたかどうかを確認することができる。さらに，受信者２１１は，正当な受領書を送付した後でしか暗号文を復号して電子情報の正しい内容を知ることができないため，電子情報を受け取ったにもかかわらず，受け取っていないと虚偽の申し出をすることもできない。また，送信者２１０と配送者２１２，および配送者２１２と受信者２１１，との間のデータのやり取りは，使用するネットワークアプリケーションに依存しないので，上記処理（ユーザデータの送受信）が可能なネットワークアプリケーションであれば，どのようなものでも使用可能である。加えて，配送者２１２は，いつ，誰と誰の間で，どのような電子情報が送られたかということを示す利用履歴を保管しているので，事後になって何らかのトラブルが発生したときに該利用履歴を提示することができる。

【００３１】つぎに，本実施形態におけるより実際的な処理の流れを，図6から図8に示す。図6は、手順１として、送信者と配送者間で行われる配達受付に関する処理を示すものである。○付き数字は、当手順内における処理順序を示す。この図において、受付証明書は，たとえば下式のとおり作成する。

受付証明書 ： Sign（配送者、証明書種別 || シリアル番号 || 配送者名 ||確定日付 || 電子情報のハッシュ値 || 送信者名）

図7は、手順２として、配送者と受信者との間で行われる配達に関する処理を示すものである。○付き数字は、当手順内における処理順序を示す。この図において、受領書は，たとえば下式のとおり作成する。

受領書 ： Sign（受信者、証明書種別 || シリアル番号 || 暗号化電子情報のハッシュ値 || 受信者名）

この式において、上記説明で述べた，「受け取った日時」に関する情報を用いても良い。

【００３２】図8は，手順３として、送信者と配送者との間で行われる配達完了通知に関する処理を示すものである。○付き数字は、当手順内における処理順序を示す。この図において、配達証明書は，たとえば下式のとおり作成する。

配達証明書 ： Sign（配送者、証明書種別 || シリアル番号 || 配送者名 ||配達日時 || 受領書）

なお，上記各式におけるSign(A，X)は，Xに対するAのディジタル署名を求めることであり、Y || ZはYとZを連結することを意味する。

【００３３】なお、上記手順において、受付証明書は、配送者が電子情報を受け取ったことを証明するものであり、配達証明は、上記実施形態において配送者から送信者へ返送される、受信者の受領書に相当するものである。

【００３４】次に，本発明の他の実施形態が適用された到達確認サービスシステムについて説明する。本実施形態が適用された到達確認サービスシステムの概略構成は，基本的に第一の実施形態の図２と同様である。また，利用者が使用する端末２００のハードウェア構成は，基本的に第一の実施形態の図３と同様である。ただし，メモリ３０６に一時的に格納される到達確認サービスプログラム３０６ｃの機能が異なる。本実施形態の到達確認サービスプログラム３０６ｃは，電子情報から専用ビューアプログラムを生成したり，受領書の正当性を検証したりするためのプログラムである。すなわち，配送者２１２は，到達確認プログラム３０６ｃを使って，送信者２１０から送られきた電子情報を，受信者２１１が配送者２１２に対して受領書を送信した場合にのみ，該電子情報の正しい内容を閲覧可能とするような，当該電子情報専用のビューアプログラムを生成するとともに，受信者２１１から送られてきた受領書の正当性を検証する。

【００３５】次に，本実施形態の到達確認サービスシステムの動作について説明する。図５は，送信者２１０が生成した電子情報を受信者２１１に送り，当該電子情報に対する受領書の受け取る場合の，送信者２１０，受信

者２１１，および配送者２１２の動作を説明するための図である。ここで，受領書とは，受信者２１１が確かに電子情報を受け取ったことを保証するデータであり，例えば，受け取った専用ビューアプログラムの圧縮子と受け取った日時とを連結したデータに受信者のディジタル署名を付加したものである。しかし，本発明はこれに限定されず，別のデータを用いてもよい。図５において，送信者２１０が行う処理には端末220_1が使用され，受信者２１１が行う処理には端末220_2が使用される。また，配送者２１２が行う処理には端末220_3が使用される。

【００３６】まず，送信者２１０は，アプリケーションプログラムを使って，受信者２１１に伝達する電子情報を生成し（ステップ４００），該電子情報と受信者２１１の宛先とを配送者２１２に送信する（ステップ４０１）。

【００３７】電子情報を受け取った配送者２１２は（ステップ４０２），到達確認サービスプログラムを使って，当該電子情報のための専用ビューアプログラムを生成する（ステップ５００）。次に，アプリケーションプログラムを使って，該専用ビューアプログラムを受信者２１１に送信する（ステップ５０１）。ここで，専用ビューアプログラムは，送信者２１０から送られてきた電子情報と，該電子情報を端末の表示装置に表示するかどうかを制御するプログラムと，受信者２１１が受領書を生成するためのプログラムと，から構成されるものであり，後述の手順が正しく実行された場合にのみ，受信者２１１が電子情報の正しい内容を知ることができるよう，該電子情報は専用ビューアプログラム内部に隠蔽されている。

【００３８】専用ビューアプログラムを受け取った受信者２１１は（ステップ５０２），該専用ビューアプログラムを起動して受領書を生成した後（ステップ４０６），アプリケーションプログラムを使って，該受領書を配送者２１２に送信する（ステップ４０７）。

【００３９】受領書を受け取った配送者２１２は（ステップ４０８），まず，到達確認サービスプログラムを使って，該受領書の正当性を検証する（ステップ４０９）。そして，該受領書が正当なものであることが確認された場合にのみ，アプリケーションプログラムを使って，確認通知を受信者２１１に送信するとともに（ステップ５０３），受領書を送信者２１０に送信する（ステップ４１３，ステップ４１４）。さらに，上記処理が行われたことを示す利用履歴を，利用履歴ファイルに保管する。ここで，受領書の正当性確認とは，該受領書が受信者本人によって生成されたものであること，および受信日時が妥当なものであること，などを確認することである。上記手順において，もし，あらかじめ決められた時間を経過した後になっても受信者２１１から受領書が送られてこなかったり，また，送られてきた受領書が正当なものでなかったりした場合には，受信者２１１にその旨を連絡して受領書の送信（再送）を要求してもよいし，送信者２１０に正当な受領書が送られてこなかった旨を連絡してもよい。

【００４０】最後に，確認通知を受け取った受信者２１１は（ステップ５０４），再び専用ビューアプログラムを起動し，該専用ビューアプログラムに確認通知を渡して電子情報を閲覧する（ステップ５０５）。上記手順では，専用ビューアプログラムを使って電子情報を閲覧するようにしているが，本発明はこれに限定されない。例えば，専用ビューアプログラムは，電子情報を閲覧可能な状態に復元する処理だけを行い，電子情報の閲覧はアプリケーションプログラムを使って行うようにしてもよい。

【００４１】また，上記手順では，受信者２１１と配送者２１２との間で，アプリケーションプログラムを使用して，受領書と確認通知とをやり取りしているが，専用ビューアプログラムと到達確認サービスプログラムが連動することによって自動で行うようにすると，受信者２１１の操作が減って便利である。上記の本実施形態では，第一の実施形態の特徴に加えて，送信者２１０と受信者２１１が到達確認サービスプログラムといった特別のソフトウェアをインストールしておく必要がないといった特徴もある。

【００４２】なお，本発明は上記各実施例に限定されるものでなく，その要旨の範囲内で様々な変形が可能である。例えば，各実施例では，ネットワークを介して送られる電子情報などの安全性は考慮していない。しかし，暗号や認証といったセキュリティ技術を使って，該電子情報を保護してもよいのは自明である。また，各実施例では，配送者が受信者に暗号文や専用ビューアプログラムを送信するときに，他の情報を併せて送ったりはしていない。しかし，本発明はこれに限定されない。例えば，該暗号文や専用ビューアプログラムと，その後に受信者より送られてくる受領書との対応関係をつけるために，識別番号などを併せて送るようにすると便利である。さらに，各実施例では，システムを利用する全てのユーザが信頼する配送者を介して電子情報のやり取りを行っているが，送信者が信頼できる場合には、配送者が行っていた処理を送信者が行うことにより，送信者と受信者の二者間で前記手順を実行するようにしてもよい。

【００４３】

【発明の効果】以上説明したように，本発明によれば，送信者が受信者に対し，ネットワークを介して電子情報を送信した場合に，受信者が当該電子情報を受け取ったことを，送信者が確認することができる。

【図面の簡単な説明】

【図１】従来の到達確認方法の概要を説明するための図である。

【図２】本発明が適用された到達確認サービスシステム

の概略構成を示す図である。

【図３】図２に示す端末のハードウェア構成を示す図である。

【図４】本発明の第一の実施形態が適用された到達確認サービスシステムにおいて，送信者が生成した電子情報を受信者に送り，当該電子情報に対する受領書を受け取る場合の送信者，受信者，および配送者の処理の流れを説明するためのフロー図である。

【図５】本発明の他の実施形態が適用された到達確認サービスシステムにおいて，送信者が生成した電子情報を受信者に送り，当該電子情報に対する受領書を受け取る場合の送信者，受信者，および配送者の処理の流れを説明するためのフロー図である。

【図６】本発明の第一の実施形態が適用された到達確認サービスシステムにおいて，送信者と配送者との間で行われる，配達受付にかかわるより実際的な処理の流れを示すフロー図である。

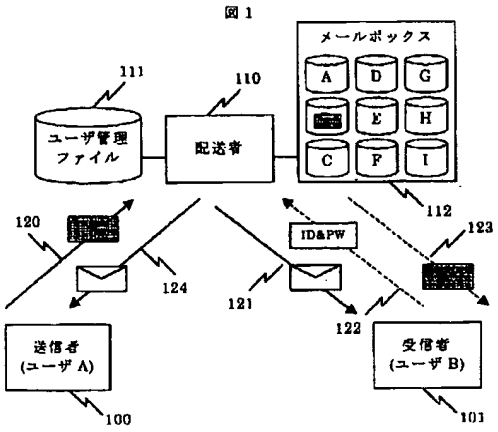
【図７】本発明の第一の実施形態が適用された到達確認サービスシステムにおいて，配送者と受信者との間で行われる，配達にかかわるより実際的な処理の流れを示すフロー図である。

【図８】本発明の第一の実施形態が適用された到達確認サービスシステムにおいて，送信者と配送者との間で行われる，配達完了通知にかかわるより実際的な処理の流れを示すフロー図である。

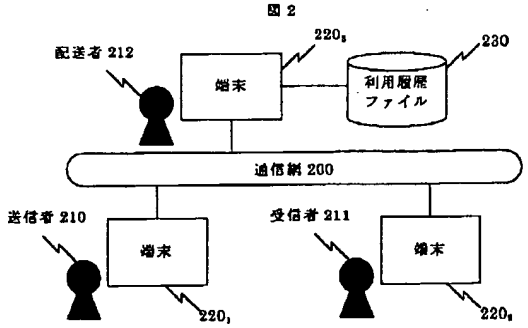
【符号の説明】

２００：通信網
２１０：送信者
２１１：受信者
２１２：配送者
２２０（220_1～220_3）：端末
２３０：利用履歴ファイル
３００：バス
３０１：表示装置
３０２：入力装置
３０３：通信網インタフェース
３０４：記憶装置
３０５：ＣＰＵ
３０６：メモリ
３０６ａ：オペレーティングシステム
３０６ｂ：アプリケーションプログラム
３０６ｃ：到達確認サービスプログラム

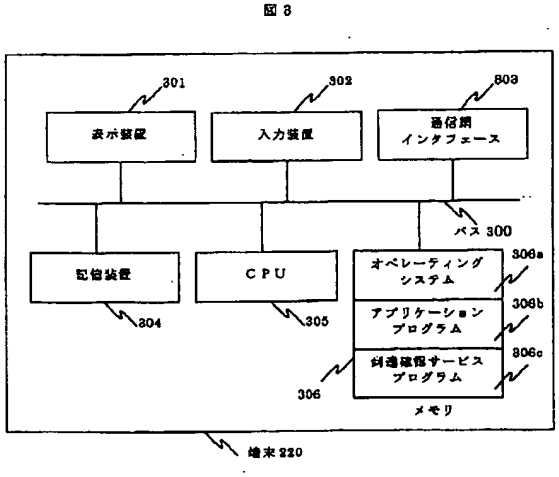
【図１】



【図２】



【図３】



【図４】

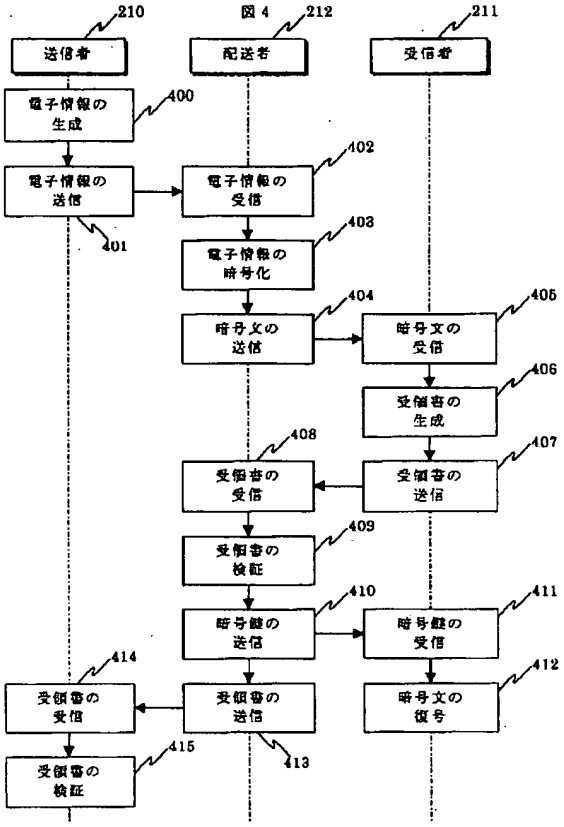


図 4
210
212
211
送信者
配送者
受信者
電子情報の生成
400
電子情報の送信
401
電子情報の受信
402
電子情報の暗号化
403
暗号文の送信
404
暗号文の受信
405
受領書の生成
406
受領書の送信
407
受領書の受信
408
受領書の検証
409
暗号鍵の送信
410
暗号鍵の受信
411
暗号文の復号
412
受領書の送信
413
受領書の受信
414
受領書の検証
415

【図５】

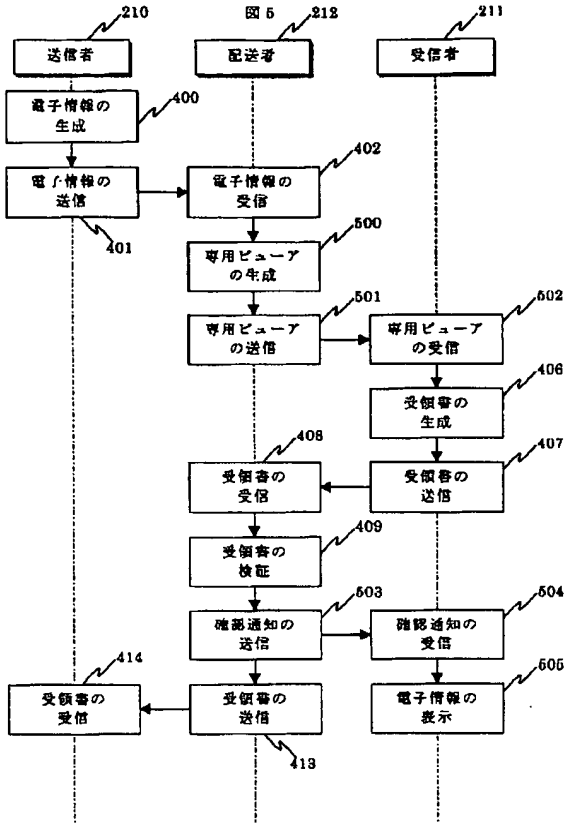
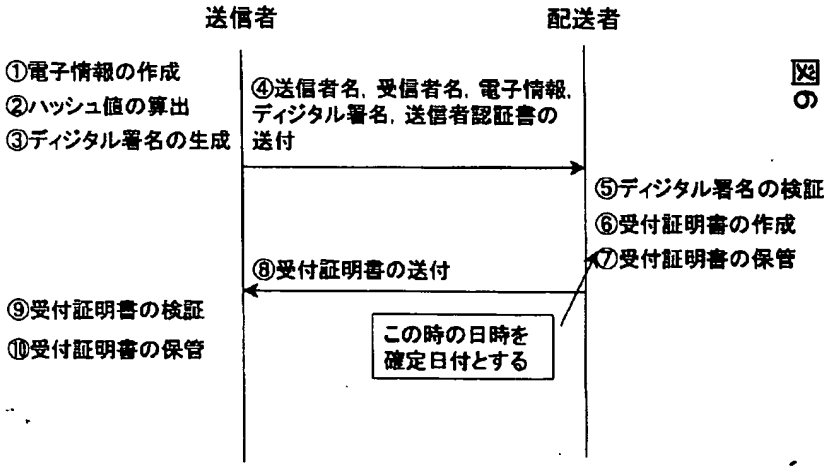


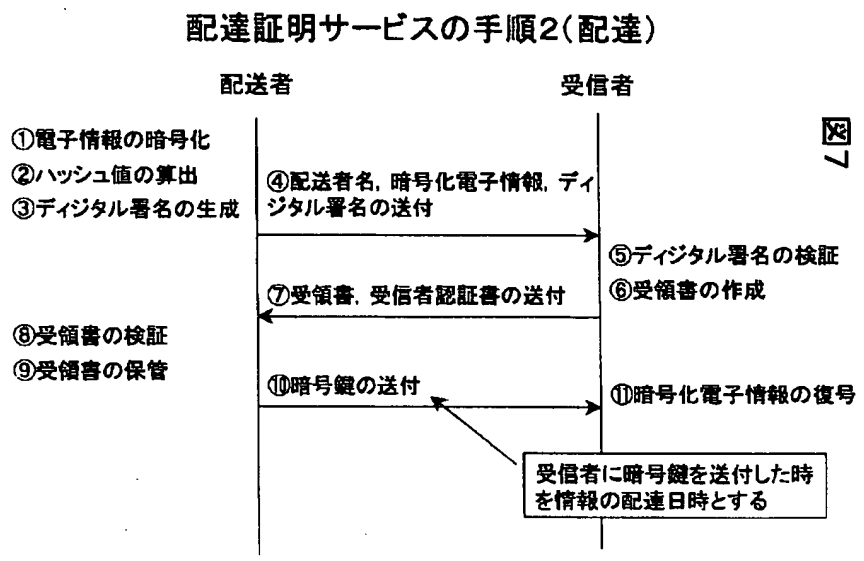
図 5
210
212
211
送信者
配送者
受信者
電子情報の生成
400
電子情報の送信
401
電子情報の受信
402
専用ビューアの生成
500
専用ビューアの送信
501
専用ビューアの受信
502
受領書の生成
406
受領書の送信
407
受領書の受信
408
受領書の検証
409
確認通知の送信
503
確認通知の受信
504
受領書の送信
413
受領書の受信
414
電子情報の表示
505

【図６】

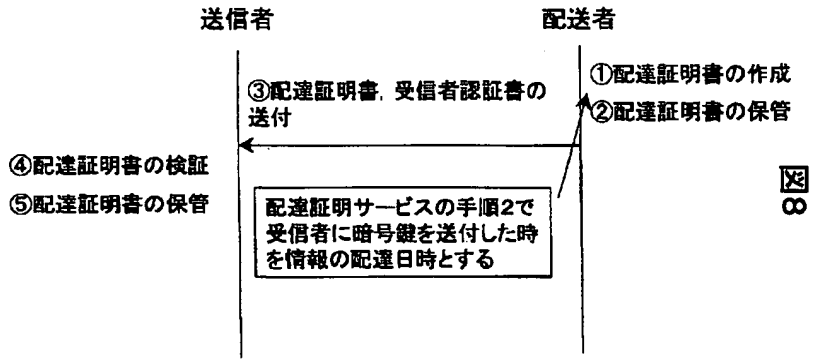

配達証明サービスの手順1（配達受付）
送信者
配送者
①電子情報の作成
②ハッシュ値の算出
③ディジタル署名の生成
④送信者名，受信者名，電子情報，ディジタル署名，送信者認証書の送付
⑤ディジタル署名の検証
⑥受付証明書の作成
⑦受付証明書の保管
⑧受付証明書の送付
⑨受付証明書の検証
⑩受付証明書の保管
この時の日時を確定日付とする

図の

【図７】



【図８】



フロントページの続き

(72)発明者　豊田　英樹
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内

(72)発明者　長野　裕美
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内

Ｆターム(参考)　5B089 GA11 GA21 GB03 JA31 KA17 KB13 KC57 KE02 KH30 LA07 LA13
5K030 GA11 GA15 HA06 KA17 LD13